UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/912,389	07/26/2001	Neil Andrew Cowie	00.177.01	5037

7590 04/16/2007

Zilka-Kotab, PC
P.O. Box 721120
San Jose, CA 95172-1120

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/16/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

Office Action Summary	**Application No.** 09/912,389	**Applicant(s)** COWIE ET AL.
	Examiner Matthew T. Henning	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 17 January 2007.

2a)☐ This action is **FINAL.** 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *See Continuation Sheet* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *See Continuation Sheet* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 30 October 2001 is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 1/17/2007.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 1/17/2007 has been entered.

Response to Arguments

Applicants' arguments filed 1/17/2007 have been fully considered but are moot in view of the new grounds of rejection presented below.

Claims 1-3, 5-8, 12, 14-19, 21-24, 28, 30-35, 37-40, 44, 46-51, 53-56, 60, 62-67, 69-72, 76, 78-83, 85-88, 92, 94-96, and 98 have been examined, while claims 4, 9-11, 13, 20, 25-27, 29, 36, 41-43, 45, 52, 57-59, 61, 68, 73-75, 77, 84, 89-91, 93, and 97 have been cancelled.

All objections and rejections not set forth below have been withdrawn.

Any claim not specifically mentioned above has been rejected by virtue of its dependency to a specifically mentioned claim.

Claim Objections

Claim 3 is objected to because of the following informalities:

Line 2 recites "said resource data of said packed computer file comparing logic" which lacks antecedent basis in the claim language. The examiner will assume that this was meant to read "said resource data comparing logic" as is consistent with claim 1.

Line 3 recites "said resource data" which has multiple antecedent basis in the claim. It is unclear to which resource data this is referring and therefore the ordinary person skilled in the art would not be able to determine the scope of the claim. For purposes of searching prior art, the examiner will assume that the limitation was meant to read "said resource data of said packed computer file" as is consistent with the rest of the claims.

Appropriate correction is required.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> *A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.*

Claims 1-3, 5-8, 12, 14-19, 21-24, 28, 30-35, 37-40, 44, 46-51, 53-56, 60, 62-67, 69-72, 76, 78-83, 85-88, 92, 94-96, and 98 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cozza (US Patent Number 5,649,095), and further in view of Arnold et al. (US Patent Number 5,442,699), hereinafter referred to as Arnold, and further in view of Pietrek ("Peering Inside the PE: A Tour of the Win 32 Portable Executable").

Regarding claims 1, 17, 33, 49, 65, and 81, Cozza disclosed a system, method, and computer program product in a computer storage medium (See Cozza Claims and Col. 1 Lines 26-33) comprising a computer program operable to control a computer to detect a known computer program within a packed computer file, said packed computer file being unpacked upon execution, said computer program comprising (See Cozza Abstract and Col. 3 Paragraph 6): resource data reading logic for reading resource data within said packed computer file (See Cozza Col. 6 Lines 21-23 and 29-34), said resource data specifying program resource items used by said known computer program (See Cozza Col. 2 Paragraph 7) and readable by a computer operating system without dependence upon which unpacking algorithm is used by said packed computer file (See Cozza Col. 6 Paragraphs 2-3 wherein the compressed file is not decompressed in order to read the resource forks information); and resource data comparing logic for generating characteristics of said resource data (See Cozza Col. 1 Lines 58-65 wherein it was inherent that the characteristic data was generated in order for the data to have been compared) and for comparing said characteristics of said resource data with characteristics of resource data of said known computer program (See Cozza Col. 7 Lines 35-39 and Col. 1 Lines 58-65) and for detecting a match with said known computer program indicative of said packed computer file containing said known computer program (See Cozza Col. 7 Lines 35-39 and Col. 1 Lines 58-65), wherein said resource data of said packed computer file is processed to generate fingerprint data (See Cozza Fig. 5); wherein said generated fingerprint data includes a number of program resource items specified within said resource data of said packed computer file (See Cozza Fig. 5 RESFORKLEN); wherein said generated fingerprint data includes a flag indicating which data is included within said generated fingerprint data (See Cozza Fig. 5); wherein the fingerprint data includes a location within said resource data of an entry specifying a program resource item having a largest size (See Cozza Col. 6 Lines 29-45); wherein said generated fingerprint data includes a checksum value of the computer file (See Cozza Fig. 5), but Cozza failed to disclose wherein said generated fingerprint data is compared with fingerprint data of said known computer program; or that the checksum value was calculated in dependence upon: a number of said program resource items specified beneath each node within hierarchically arranged resource data of said packed computer file; string names associated with said program resource items within said resource data of said packed computer file; and sizes of said program resource items within said resource data of said packed computer file. However, Cozza did disclose the file including a number of program resource items specified within said resource data (See Cozza Col. 2 Paragraph 7).

Pietrek teaches that a Win32 PE file is an executable file which contains un-initialized code and resources, which when executed the code is initialized using the resources (See Pietrek Page 21 PE File Base Relocations).

Arnold teaches a method of virus scanning in which hashes of a file are created and compared to hashes of known viral patterns in order to detect computer viruses upon matching (See Arnold Col. 10 Lines 48-52).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Pietrek in the virus detector of Cozza by allowing the scanning of Win32 PE files and their resources. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide protection against Win32 PE files containing viruses.

It further would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Arnold in the virus scanning of Cozza by creating hashes of the data, including the resources, of the compressed file and comparing it to hashes of known viral patterns. This would have been obvious because the ordinary person skilled in the art would have been motivated to scan the files as quickly as possible, without compromising security.

It would have been obvious in this combination that because the file contains the resource fork and resource items, and the hash is taken of the file, the signature includes a number of resource items specified within the resource fork. It further would have been obvious that because the fingerprint data represented the file during comparison, and the flags of Cozza indicated the viruses found in the file, the fingerprint data would have included a flag indicating which data (viruses) was included within said fingerprint data.

It further would have been obvious that the checksum of the file in this combination would have been dependant upon a number of said program resource items specified beneath each node within hierarchically arranged resource data of said packed computer file; string names associated with said program resource items within said resource data of said packed computer file; and sizes of said program resource items within said resource data of said packed computer file, as Pietrek teaches that Win32 PE files are arranged in such a manner, as is seen is Pietrek Fig. 5 and Table 13.

Regarding claims 2, 18, 34, 50, 66, and 82, Cozza, Arnold, and Pietrek disclosed that said known computer program is one of: a Trojan computer program; and a worm computer program (See Cozza Col. 1 Lines 22-32 and Col. 7 Lines 35-39).

Regarding claims 3, 19, 35, 51, 67, and 83, Cozza, Arnold, and Pietrek disclosed that said resource data comparing logic is operable to compare said resource data with characteristics of a plurality of known computer programs to detect if said packed computer program contains one of said plurality of known computer programs (See Cozza Col. 7 Lines 35-40).

Regarding claims 5, 21, 37, 53, 69, and 85, Cozza, Arnold, and Pietrek disclosed that said program resource items used by said known computer program include one or more of: icon data; string data; dialog data; bitmap data; menu data; and language data (See Cozza Col. 2 Paragraph 7).

Regarding claims 6-8, 22-24, 38-40, 54-56, 70-72, and 86-88, the combination of Cozza, Arnold, and Pietrek disclosed specifying a storage location for each resource item as an offset, and the size of each resource (See Pietrek Page 20 Table 13 Offsets and Page 21 Fig. 14 DWORD OffsetToData).

Regarding claims 12, 28, 44, 60, 76, and 92, Cozza, Arnold, and Pietrek disclosed that said generated fingerprint data includes timestamp data indicative of a time of compilation of said known computer program (See Cozza Fig. 5 VOLUMECRDATE).

Regarding claims 14, 30, 46, 62, 78, 94, and 98, Cozza, Arnold, and Pietrek did not specifically disclose that the checksum is rotated between each item being added into said checksum, but SHA, which shifts 1 bit to the left after each operation, was a well known checksum in the art at the time of invention, and as such it would have been obvious to the ordinary person skilled in the art to have used SHA as the checksum.

Regarding claims 15, 31, 47, 63, 79, and 95, Cozza, Arnold, and Pietrek disclosed decompressing the computer program upon execution (See Pietrek Page 21 PE File Base Relocations).

Regarding claims 16, 32, 48, 64, 80, and 96, see the rejection of claim 1 above.

Conclusion

Claims 1-3, 5-8, 12, 14-19, 21-24, 28, 30-35, 37-40, 44, 46-51, 53-56, 60, 62-67, 69-72, 76, 78-83, 85-88, 92, 94-96, and 98 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Matthew Henning
Assistant Examiner
Art Unit 2131
4/11/2007

04/17/2007
SYED ZIA
PRIMARY EXAMINER
AU 2131

Continuation of Disposition of Claims: Claims pending in the application are 1-3,5-8,12,14-19,21-24,28,30-35,37-40,44,46-51,53-56,60,62-67,69-72,76,78-83,85-88,92,94-96 and 98.

Continuation of Disposition of Claims: Claims rejected are 1-3,5-8,12,14-19,21-24,28,30-35,37-40,44,46-51,53-56,60,62-67,69-72,76,78-83,85-88,92,94-96 and 98.